A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports tc business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.

1

CONF-850723--2

LA-UR -85-828

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

TITLE NEW PROBABILISTIC MODELING AND SIMULATION METHODS FOR COMPLEX TIME-DEPENDENT SYSTEMS

LA-UR--85-828

AUTHOR(S) Robert J. Bartholomew, WX-11

DE85 009575

SUBMITTED TO Seventh International System Safety Conference

MASTER

Los Alamos Los Alamos National Laboratory
Los Alamos, New Mexico 87545

FORM NO. 836 R4

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

New Probabilistic Modeling and Simulation Methods for Complex Time-Dependent Systems

Robert J. Bartholomew, Ph.D., PE; Los Alamos National Laboratory; Los Alamos, NM

Abstract

This paper is a tutorial that presents a new method of modeling the probabilistic description of failure mechanisms in complex, time-dependent systems. The method of modeling employs a state vector differential equation representation of cumulative failure probabilities derived from Markov models associated with certain generic fault trees, and the method automatically includes common cause/common mode statistical dependencies, as well as time-related dependencies not considered in the literature previously. Simulations of these models employ a population dynamics representation of a probability space involving probability particle transitions among the Markov disjoint states. The particle transitions are governed by a random, Monte Carlo selection process.

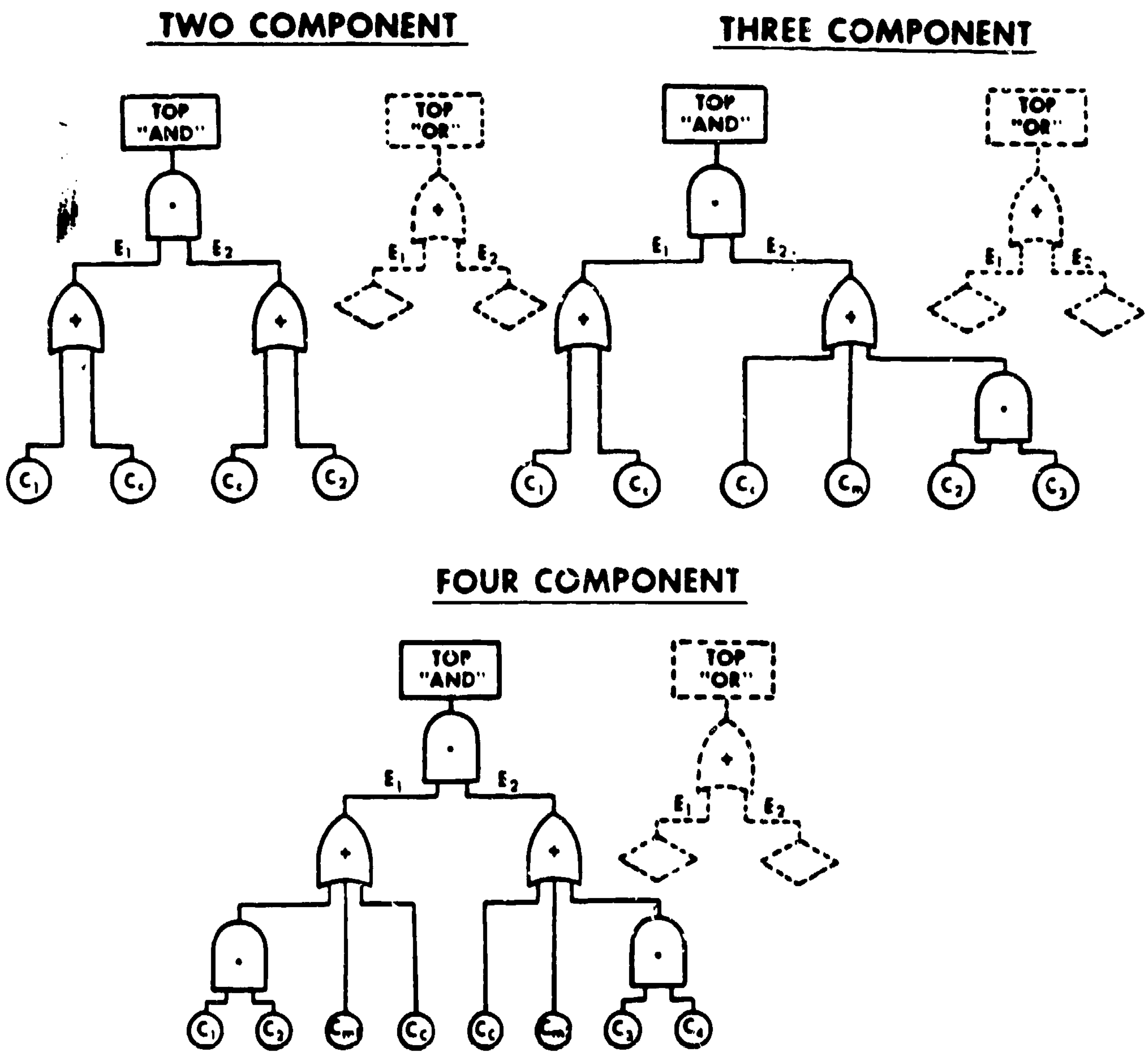
Introduction

The calculation of the probability of failure occurrence in systems that comprise many diverse components generally uses Fault Tree Analysis (FTA) as a final step to identify failure mechanisms and logically structure their paths in a graphical, formalized manner. A necessary second step for quantitative probability analysis involves assigning occurrence probabilities (or rates) to each of the basic events in the fault tree that singly, or in combination, result in top event (or system failure) occurrence. For time-dependent systems, the calculation of occurrence probabilities can be performed by a stochastic process theory model known as the Markov model (Ref. 1). This tutorial paper describes a formalized new method known as the Failure Mode State Variable (FMSV) method employing generic fault trees and the mathematical structure of modern state variable theory to describe how several practical systems can be analyzed. Monte Carlo simulation of the Markov models employing probability particle transitions are developed. A synthesis of generic fault trees is employed to approximate top event occurrence rates for subsystem fault trees that are used for a complete system probabilistic failure probability calculation. Several practical examples drawn from nuclear safety and safeguards systems that illustrate the methods are presented.

Method

Failure Mode State Variable (FMSV) Formulation: Three generic fault trees each having two failure models (inputs to the top gate) comprising two, three, or four statistically independent (s-independent) initiators together with common cause and/or common mode s-independent initiators were developed. These fault trees are shown in Fig. 1. The Markov state transition graphs for three kinds of two component fault trees are shown in Fig. 2, and a three identical component merged to a two component system is shown in Fig. 3. The

EDB



$C_i \equiv$ ith CAUSE, $C_c \equiv$ COMMON CAUSE,

$C_{mi} \equiv$ ith COMMON MODE, $E_i \equiv$ ith EFFECT

Fig. 1. Generic Fault Trees for up to four numbered initiators (components) and with common cause and/or common mode initiators.

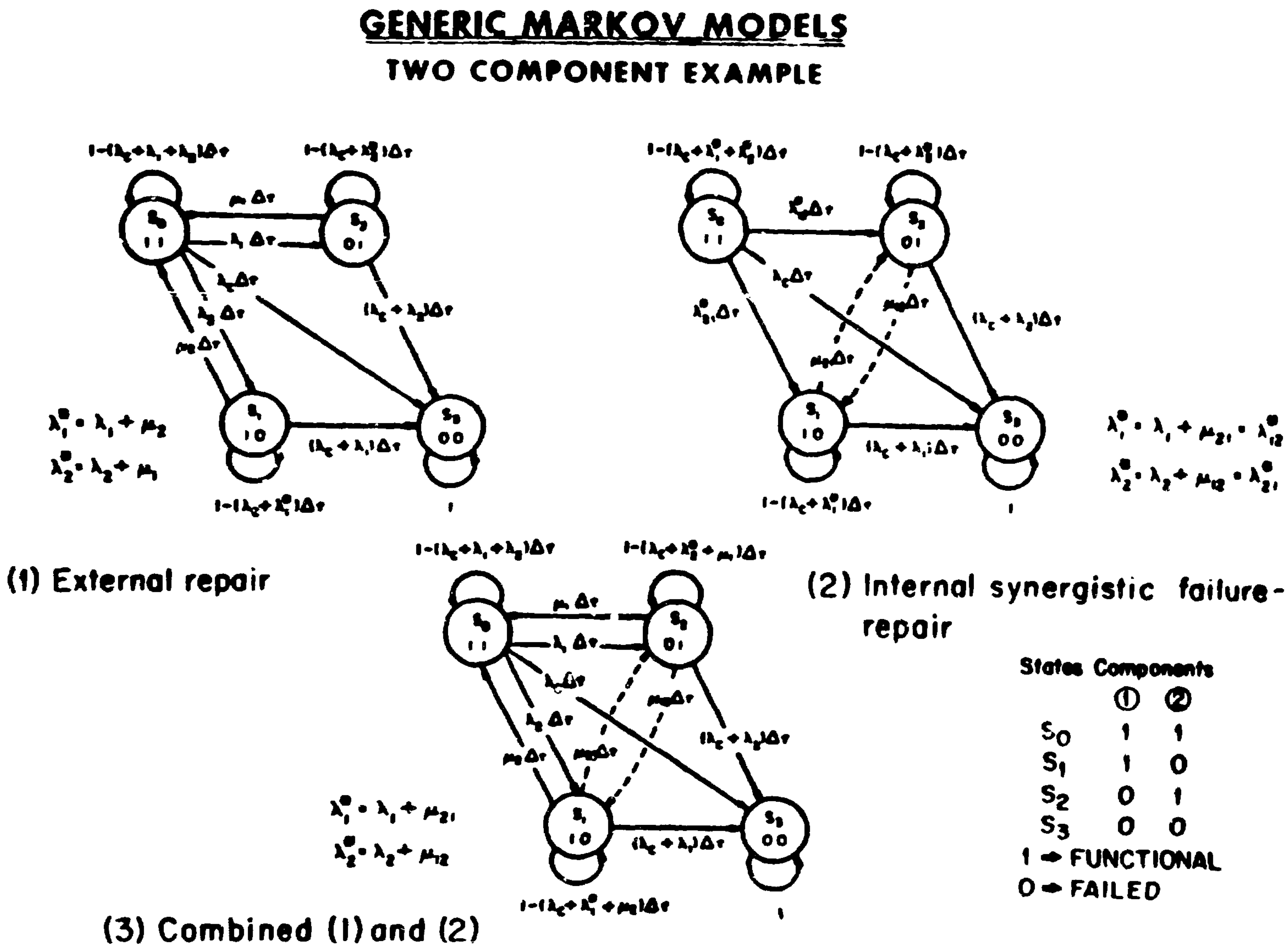


Fig. 2. Generic Markov models for two numbered initiator Fault Tree with common cause and involving three kinds of time-dependent failure/repair mechanisms.

MERGING OF MARKOV MODEL STATES

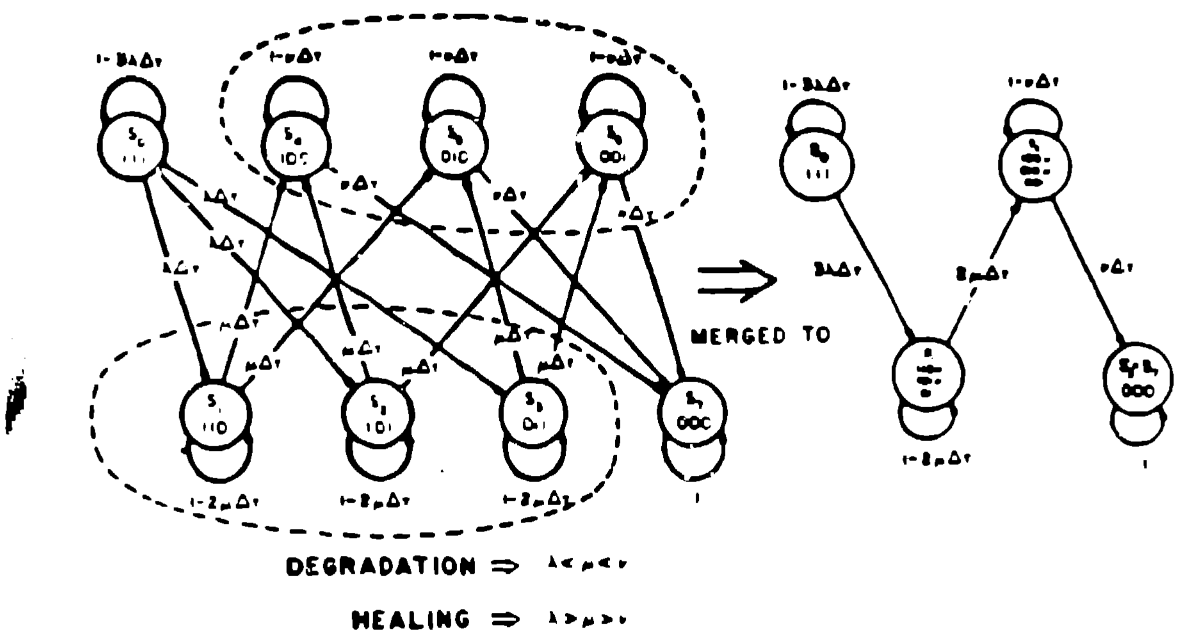


Fig. 3. Three identical component Markov models merged to four state equivalent two component model describing "jump" conditional failure rate time dependency.

disjoint nature of the Markov states allows one to formulate a transformation matrix $\underline{E}$ consisting of only zero's and one's to transform the probability (P_i) of being in a given Markov state (S_i; $i = 0, 1, \cdots, 2^n - 1$) into the probability ($\hat{P}_i$) of none, one, or more combinations of initiator occurrences described by finite unions of the Markov states (Ref. 2). This set of unions of Markov states (S_i) is called a set of Adjoint states ($\hat{S}_i$); $i = 0, 1, \cdots, 2^n - 1$) and comprises successive unions of the S_i in which all combinations of occurrences of basic events (not common cause or common mode) are depicted. By "common cause" is meant a basic event or s-independent union of basic events that singly cause the top event to occur. By "common mode" is meant a basic event or s-independent union of basic events that singly cause a defeat of redundancy in a system. The $\hat{S}_0$ Adjoint state is chosen to represent S_m ($m = 2^n - 1$), the occurrence of all n basic events. The $\hat{S}_m$ Adjoint state is chosen to represent the union of all of the S_i and is designated (Ω). The intermediate $\hat{S}_i$; $i = 1, 2, \cdots, m - 1$ represent all of the combinations of occurrences of any one, any two, etc., basic events. The resulting transformation matrix $\underline{E}$ is one-to-one and a 2^nth-order Markov model comprising n components and of the form:

$$d\underline{P}/dt \equiv \dot{\underline{P}}(t) = \underline{A}\,\underline{P}(t),\ t > 0\ ;\ \underline{P}(0) \quad , \tag{1}$$

is transformed to the Adjoint state model

$$d\hat{\underline{P}}/dt \equiv \dot{\hat{\underline{P}}}(t) = \hat{\underline{A}}\,\hat{\underline{P}}(t),\ t > 0;\ \hat{\underline{P}}(0) \quad , \tag{2}$$

by the similarity transformation

$$\hat{\underline{A}} = \underline{E}\,\underline{A}\,\underline{E}^{-1} \quad . \tag{3}$$

Now, because the generic fault tree Markov models each have an absorbing state represented by S_m (all numbered initiators have occurred), the last column of matrix $\underline{A}$ is a column of zero's; whereas, the last row of matrix $\hat{\underline{A}}$ is a row of zero's, which establishes $\hat{P}_m(t) = 1$, $t > 0$. In words, this establishes the certainty of being in one of the complete set of Markov states at any time (t). It can also be shown that $P_m(t)$ also represents the probability of occurrence in [0,t] of each and every failure mode (inputs to a top "AND" gate) of a given system (Ref. 2).

Given that the occurrence of each numbered basic event (as well as common cause/common mode events) follows an exponential distribution for the "waiting time" between events, by reordering the $\hat{P}_i$ so that the vector $\hat{P}$ represents the occurrence of each single (numbered) coupled basic event, each double, each triple, etc., with $\hat{P}_m(\ )$ eliminated from the system one obtains the Failure Mode State Variable (FMSV) inhomogeneous system:

$$d\underline{F}/dt \equiv \dot{\underline{F}} = \underline{A}'\ \underline{F} + \underline{B}\ \underline{u}(t),\ t > 0;\ F(0)$$

$$\underline{T}(t) = \underline{C}\ \underline{F} + \underline{D}\ \underline{u}(t) \quad , \tag{4}$$

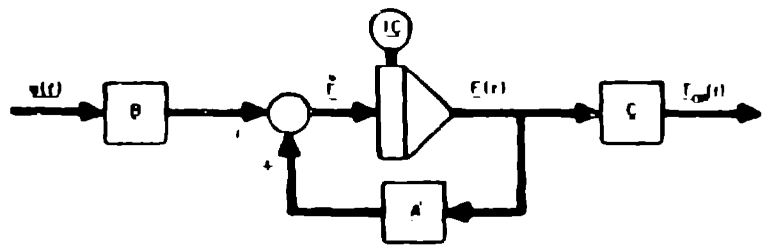
which is in the general mathematical form for a state variable feedback control system where $\underline{u}(t)$ represent the system "inputs" (basic event lifetime cumulative distribution functions - lcdf's) that are known, $\underline{F}(t)$ are the system state variables, and $\underline{T}(t)$ represent the system "outputs" that are the lcdf's of the top "OR" gate output or other combinations of failure mode occurrences representing system failures of one kind or another. Figure 4 shows the analog state variable generalized simulation diagram and the matrices $\underline{A}'$, $\underline{B}$, and $\underline{C}$ for the four kinds of two component systems described by the Markov transition matrices of Figs. 2 and 3 ($\underline{D} = \underline{0}$ for these models). The seventh order FMSV model with internal synergistic failure mode coupling for the three component generic fault tree is shown in Fig. 5. The fifteenth order four component model has the same form but is not shown for the sake of brevity. These models illustrate the generality of models for systems having two, three, and four numbered initiators with additional common cause/common mode initiators. (Note that the number of common cause/common mode initiators does not increase the order of the systems.)

Monte Carlo Simulation: Although the FMSV models can be solved as any deterministic system, and yield exact solutions or numerically accurate solutions that are the lcdf's of the system, only a restricted class of problems can be solved in closed form. It is readily shown that when failure or repair rates in a system change with time (for example, the classic bathtub hazard rate curve), the solution of the FMSV system becomes more difficult. If it can be postulated that these rates are interdependent such that they depend on relationships that lead to a nonlinear FMSV model, deterministic solutions become much more difficult. The beauty of the Monte Carlo simulation involving random process sampling is that a nonconstant rate or nonlinearity is no harder to solve than a linear system. Also, if one begins with the Markov states and uses population dynamics to represent particle transitions, a system can be approximated without going through the step of developing the Markov or FMSV differential equations.

TWO COMPONENT EXAMPLE

FAILURE MODE STATE VECTOR (FMSV) MODELS

FMSV model of the form $\dot{\underline{F}} = \underline{A}'\underline{F} + \underline{B}\,\underline{u}(t);\ \underline{F}(0);\ T_{on}(t)$



(1) External repair

$$\underline{A}' = \begin{bmatrix} -(\lambda_c+\lambda_1') & 0 & \mu_1 \\ 0 & -(\lambda_c+\lambda_2') & \mu_2 \\ \lambda_2 & \lambda_1 & -(\lambda_c+\lambda_1+\lambda_2) \end{bmatrix}$$

$$\underline{B} = \begin{bmatrix} (\lambda_c+\lambda_1) & 0 & 0 & 0 \\ (\lambda_c+\lambda_2) & 0 & 0 & 0 \\ \lambda_c & 0 & 0 & 0 \end{bmatrix}$$

$\underline{C} = [1 \quad 1 \quad -1]$

$\lambda_1' = \lambda_1+\mu_1,\ \lambda_2' = \lambda_2+\mu_2$

(2) Internal synergistic failure-repair

$$\underline{A}' = \begin{bmatrix} -(\lambda_c+\lambda_1^*+\mu_{12}) & 0 & \mu_{12} \\ 0 & -(\lambda_c+\lambda_2^*+\mu_{21}) & \mu_{21} \\ \lambda_2 & \lambda_1 & -(\lambda_c+\lambda_1+\lambda_2) \end{bmatrix}$$

$$\underline{B} = \begin{bmatrix} (\lambda_c+\lambda_1^*) & 0 & 0 & 0 \\ (\lambda_c+\lambda_2^*) & 0 & 0 & 0 \\ \lambda_c & 0 & 0 & 0 \end{bmatrix}$$

$\underline{C} = [1 \quad 1 \quad -1]$

$\lambda_1^* = \lambda_1+\mu_{21},\ \lambda_2^* = \lambda_2+\mu_{12}$

(3) Combined (1) and (2)

$$\underline{A}' = \begin{bmatrix} -(\lambda_c+\lambda_1'+\mu_{12}) & \mu_{21} & (\mu_1+\mu_{12}-\mu_{21}) \\ \mu_{12} & -(\lambda_c+\lambda_2'+\mu_{21}) & (\mu_2+\mu_{21}-\mu_{12}) \\ \lambda_2 & \lambda_1 & -(\lambda_c+\lambda_1+\lambda_2) \end{bmatrix}$$

$$\underline{B} = \begin{bmatrix} (\lambda_c+\lambda_1) & 0 & 0 & 0 \\ (\lambda_c+\lambda_2) & 0 & 0 & 0 \\ \lambda_c & 0 & 0 & 0 \end{bmatrix}$$

$\underline{C} = [1 \quad 1 \quad -1]$

$\lambda_1' = \lambda_1+\mu_1,\ \lambda_2' = \lambda_2+\mu_2$

$\underline{F}(t) = [F_1(t)\ F_2(t)\ T_{on}(t)]^T,\ \underline{IC} = [F_1(0)\ F_2(0)\ T_{on}(0)]^T,\ \underline{u}(t) = [1\ 1\ e^{-\lambda_c t}\ e^{-\lambda_1 t}\ e^{-\lambda_2 t}]^T$

(4) Sequential "jump" failure rate dependency among three identical components

$$\underline{A}' = \begin{vmatrix} 3\lambda & 0 & 0 \\ 2\mu & 2\mu & 0 \\ 0 & \mu & \mu \end{vmatrix}$$

$F(t) = [F_1(t)\ F_2(t)\ F_3(t)]^T,$

$IC = [F_1(0)\ F_2(0)\ F_3(0)]^T,$

$u(t) = [1\ 0\ 0]^T$

$$\underline{B} = \begin{vmatrix} 3\lambda & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{vmatrix}$$

For failure defined
(1) only one of three,
(2) only two of three, or
(3) all three,

$T_{on}(t) = [T_1(t)\ T_2(t)\ T_3(t)]^T$, and $\underline{C} = \begin{vmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{vmatrix}.$

Fig. 4. General analog simulation of Failure Mode State Vector (FMSV) models involving four kinds of time-statistical dependencies for a two-component Generic Markov model.

THREE COMPONENT FAILURE MODE STATE VARIABLE MODEL

The FMSV model of the form $\dot{\underline{F}} = \underline{A}'\underline{F} + \underline{B}\,\underline{y}(t);\ \underline{F}(0);\ T_{OR}(t)$ is:

$$
\begin{bmatrix} \dot{U}_2 \\ \dot{U}_3 \\ \dot{F}_1 \\ \dot{F}_2 \\ \dot{T}_{12} \\ \dot{T}_{13} \\ \dot{T}_{AND} \end{bmatrix}
=
\begin{bmatrix}
-(\lambda_c+\lambda_m+\lambda^{*}_{23}) & 0 & \frac{\lambda_2}{(\lambda_2+\lambda_3)}\mu_{12} & -\mu_{21} & -\frac{\lambda_2}{(\lambda_2+\lambda_3)}\mu_{12} & -\mu_{12} & (\mu_{12}+\mu_{21}) \\
0 & -(\lambda_c+\lambda_m+\lambda^{*}_{32}) & \frac{\lambda_3}{(\lambda_2+\lambda_3)}\mu_{12} & -\mu_{21} & -\mu_{12} & -\frac{\lambda_3}{(\lambda_2+\lambda_3)}\mu_{12} & (\mu_{12}+\mu_{21}) \\
0 & 0 & -(\lambda_c+\lambda^{*}_1+\mu_{12}) & 0 & \mu_{12} & \mu_{12} & -\mu_{12} \\
\lambda^{*}_{32} & \lambda^{*}_{23} & \mu_{12} & -(\lambda_c+\lambda_m+\lambda^{*}_2+\mu_{21}) & -\frac{(2\lambda_2+\lambda_3)}{(\lambda_2+\lambda_3)}\mu_{12} & -\frac{(\lambda_2+2\lambda_3)}{(\lambda_2+\lambda_3)}\mu_{12} & (\mu_{21}+2\mu_{12}) \\
\lambda^{*}_1 & 0 & (\lambda_m+\lambda_2) & -\mu_{21} & -(\lambda_c+\lambda_m+\lambda^{*}_1+\lambda_2) & 0 & \mu_{21} \\
0 & \lambda^{*}_1 & (\lambda_m+\lambda_3) & -\mu_{21} & 0 & -(\lambda_c+\lambda_m+\lambda^{*}_1+\lambda_3) & \mu_{21} \\
0 & 0 & \lambda_m & \lambda_1 & \lambda_3 & \lambda_2 & -(\lambda_c+\lambda_m+\sum_{i=1}^{3}\lambda_i)
\end{bmatrix}
\begin{bmatrix} U_2 \\ U_3 \\ F_1 \\ F_2 \\ T_{12} \\ T_{13} \\ T_{AND} \end{bmatrix}
$$

$$
+
\begin{bmatrix}
(\lambda_c+\lambda_m+\lambda^{*}_{23}) & 0 & 0 & 0 & 0 & 0 \\
(\lambda_c+\lambda_m+\lambda^{*}_{32}) & 0 & 0 & 0 & 0 & 0 \\
(\lambda_c+\lambda^{*}_1) & 0 & 0 & 0 & 0 & 0 \\
(\lambda_c+\lambda_m) & 0 & 0 & 0 & 0 & 0 \\
\lambda_c & 0 & 0 & 0 & 0 & 0 \\
\lambda_c & 0 & 0 & 0 & 0 & 0 \\
\lambda_c & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\begin{bmatrix} 1 \\ 1-e^{-\lambda_c t} \\ 1-e^{-\lambda_m t} \\ 1-e^{-\lambda_1 t} \\ 1-e^{-\lambda_2 t} \\ 1-e^{-\lambda_3 t} \end{bmatrix}
$$

$$\underline{F}(0) = \begin{bmatrix} U_2(0) & U_3(0) & F_1(0) & F_2(0) & T_{12}(0) & T_{13}(0) & T_{AND}(0) \end{bmatrix}^T$$

$$T_{OR}(t) = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 & -1 \end{bmatrix} \underline{F}(t)$$

$\lambda^{*}_1 = \lambda_1 + \mu_{21}$, $\lambda^{*}_2 = \lambda_2 + \lambda_3 + \mu_{12} = \lambda^{*}_{23} + \lambda^{*}_{32}$,
$\lambda^{*}_{23} = \lambda_2 + \lambda_3\,\mu_{12}/(\lambda_2+\lambda_3)$, $\lambda^{*}_{32} = \lambda_3 + \lambda_2\,\mu_{12}/(\lambda_2+\lambda_3)$

Fig. 5. The matrix form of the three component Generic Fault Tree and its Markov model having common cause and common mode dependencies and internal synergistic failure-repair rate dependencies.

The basis of the use of Monte Carlo techniques for simulating the generic fault tree Markov models is found in the concept of time-dependent probability P(t) as having a probability measure described by a finite, discrete number of particles whose total number is constant to preserve continuity, but these particles may migrate around various possible states of a system (Markov states). The impetus for such a description lies in the fact that some failure processes such as nucleation and growth failure (Ref. 3) can be expressed only in terms of cumulative degradation leading to intolerable or out of range system performance. The mechanisms involved may be at an atomic or molecular level, where many interactions are possible, and some of these may retard failure as well as accelerate it. Assuming that such processes can be described stochastically (as in radioactive decay), it is possible to formulate a reliability (or unreliability) model with a one-to-one correspondence between the particles involved in the degradation or healing process and the reliability (probability) particles we invent to describe the probability of the entire system remaining functional. Tagging each of these particles with a positive integer, they then occupy certain finite volume spaces described by each Markov state. The probability of one-and-only-one particle transition between any two disjoint states during the small random time interval Δt depends on the product of the transition rate (λ-failure or μ-repair) between the states and the number of particles at time t residing in the state from which the transition takes place. This concept corresponds to the classical "birth-death" population dynamics problem of stochastic process theory except that for Markov models we are conceiving of absolute probabilities of being in a Markov state instead of the relative transition probabilities associated with Markov process chains.

An example involving the two-component generic fault tree Markov model with internal synergistic failure-repair mechanisms best serves to show the process. We have the following definitions:

$\lambda_c \equiv$ common cause failure rate ,

$\lambda_i;\ i = 1,2 \equiv$ failure rates of components 1 and 2, respectively ,

$\mu_{12} \equiv$ synergistic failure-repair rate involving repair of component 1 at the expense of failure of component 2 ,

$\mu_{21} \equiv$ synergistic failure-repair rate involving repair of component 2 at the expense of failure of component 1 ,

$\lambda_1^* \equiv \lambda_1 + \mu_{21}$, and

$\lambda_2^* \equiv \lambda_2 + \mu_{12}$.

The expressions for λ_1 and λ_2 follow from birth and death process postulates where the λ_i, μ_{ij} are death and birth rates, respectively.

In the Monte Carlo simulation, we have the following complete delineation of possible single-event occurrences in a small time interval Δt.

Event	Transition
E_1	$S_0 \xrightarrow{\lambda_2^*} S_1$
E_2	$S_0 \xrightarrow{\lambda_1^*} S_2$
E_3	$S_0 \xrightarrow{\lambda_c} S_3$
E_4	$S_1 \xrightarrow{\mu_{21}} S_2$
E_5	$S_1 \xrightarrow{(\lambda_c + \lambda_1)} S_3$
E_6	$S_2 \xrightarrow{\mu_{12}} S_1$
E_7	$S_2 \xrightarrow{(\lambda_c + \lambda_2)} S_3$

To complete the list, we have nonevent E_8 corresponding to the possibility that no transition takes place during Δt from t.

If we begin the process with N_T "particles of reliability" in S_0 and none in each of the other states corresponding to the initial condition that both components are certain to function, initially, we can simulate the failure process by random sampling from a cumulative distribution function (which will be determined presently) to determine which of the eight events occur in any given Δt. If we keep track of how many particles there are at any given time t from zero time in each state, and normalize by dividing that number of particles by N_T, we have an estimate of the probability of being in each state as a function of time. To keep track of the passage of time we use the fact that because the process is Markovian (Poisson, to be specific), the waiting time between event occurrences is exponentially distributed. Thus, we can sample from the inverse of the cumulative distribution function $\phi(\Delta t) = 1 - e^{-\sigma(t)\Delta t}$, where Δt is the random time interval elapsed until the next event occurs, given that one has just occurred at time t, and $\sigma(t)$ is a function of time related to the occurrence rate representing the totality of possible event occurrences in Δt. A fundamental theorem of probability says that the inverse of a cdf is the uniform distribution. Thus, if we had a method of choosing random numbers ξ_1 between 0 and 1, we can rewrite

$$\Delta t = -\ln \xi_1 / \sigma(t) \quad ,$$

where ξ_1 is distributed uniformly on (0,1). Obviously, in the function $\ln[1 - \phi(\Delta t)]$, being uniformly distributed, it matters not where the center of the distribution is, so choosing ξ_1 from the excluded interval (0,1) will always provide a positive random Δt from the present time t.

We now formulate the event sampling cumulative distribution function. Because E_1 through E_7 represent the totality of event occurrences, Σ, and letting $\{N_0(t), N_1(t), N_2(t), N_3(t)\}$ represent the distribution of the N_T particles within and among the four states $\{S_0,S_1,S_2,S_3\}$, we have the constraint

$$N_T = N_0(t) + N_1(t) + N_2(t) + N_3(t) \quad , \text{ all } t \geq 0 \quad , \tag{5}$$

which corresponds to the Markov probability state vector theory property

$$\sum_{i=0}^{3} P_i(t) = 1 \quad , \tag{6}$$

for all t > 0. We can define an event occurrence rate function of time, $\sigma(t)$, representing the totality of possible event occurrences during any Δt from t, given that the last occurrence was exactly at time t. This definition is

$$\sigma(t) = \overset{*}{\lambda_2}N_0(t) + \overset{*}{\lambda_1}N_0(t) + \lambda_c N_0(t) + \mu_{21}N_1(t) + (\lambda_c + \lambda_1)N_1(t)$$
$$+ \mu_{12}N_2(t) + (\lambda_c + \lambda_2)N_2(t) \quad . \tag{7}$$

We can formulate a cumulative distribution function (cdf) and choose random samples ξ_2 uniform on (0,1) to determine which event occurs during the sample interval Δt during which one and only one event can occur. This cdf is formulated as follows:

$P_1(t) = \overset{*}{\lambda_2}N_0(t)/\sigma(t)$. If $0 < \xi_2 \leq P_1(t)$, E_1 occurs.

$P_2(t) = P_1(t) + \overset{*}{\lambda_1}N_0(t)/\sigma(t)$. If $P_1(t) < \xi_2 \leq P_2(t)$, E_2 occurs.

$P_3(t) = P_2(t) + \lambda_c N_0(t)/\sigma(t)$. If $P_2(t) < \xi_2 \leq P_3(t)$, E_3 occurs.

$P_4(t) = P_3(t) + \mu_{21}N_1(t)/\sigma(t)$. If $P_3(t) < \xi_2 \leq P_4(t)$, E_4 occurs.

$P_5(t) = P_4(t) + (\lambda_c + \lambda_1)N_1(t)/\sigma(t)$. If $P_4(t) < \xi_2 \leq P_5(t)$, E_5 occurs.

$P_6(t) = P_5(t) + \mu_{12}N_2(t)/\sigma(t)$. If $P_5 < \xi_2 \leq P_6(t)$, E_6 occurs.

$P_7(t) = P_6(t) + (\lambda_c + \lambda_2)N_2(t)/\sigma(t)$. If $P_6(t) < \xi_2 < 1.0$, E_7 occurs. (8)

Because the process requires that during the finite, random time interval Δt one and only one event can occur (or no event occurs), and we have delineated all of the possible, mutually exclusive events, our simulation of particle transitions during every small random time interval Δt will represent a population dynamics process. An approximate measure of the expected probability of being in any of the states S_i; i = 0,1,2,3 at discrete time points is determined from the recursion formula $t_m = t_{m-1} + \Delta t_m$; m = 1,2,···,

A SIMPLIFIED NUCLEAR REACTOR SCRAM SYSTEM WITH COMMON CAUSE CAN BE REPRESENTED BY A THREE COMPONENT GENERIC FAULT TREE

COMPARISON OF RESULTING LIFETIME CUMULATIVE DISTRIBUTION FUNCTIONS ESTABLISH EXACTNESS OF FMSY MODEL AND PROPERTIES OF MONTE CARLO SIMULATION

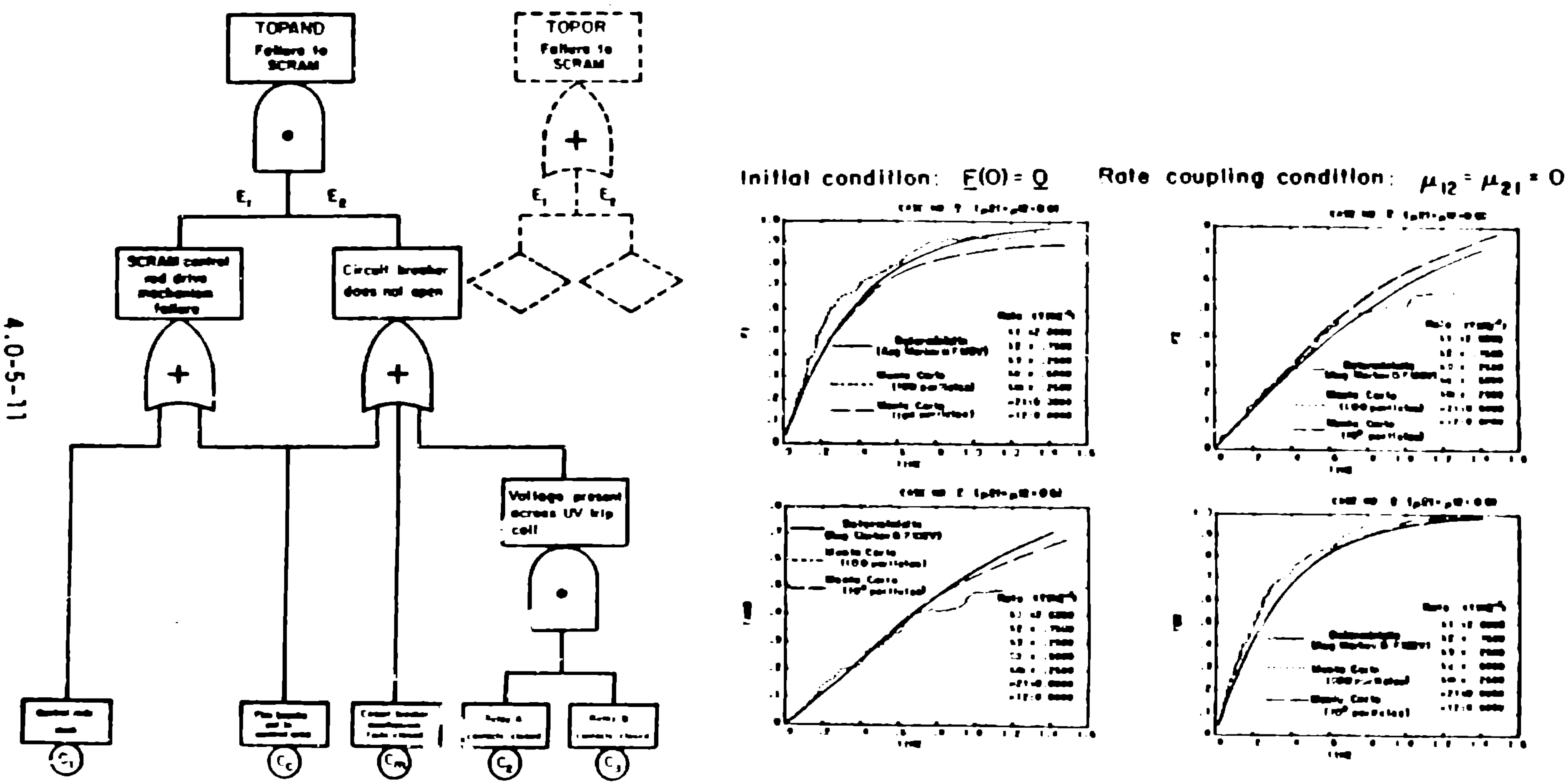


Fig. 6. Application of FMSV and Monte Carlo simulation models to a simplified nuclear reactor SCRAM system represented by a three initiator fault tree/ Markov model with a common cause and a common mode as additional initiators.

beginning at $t_0 = 0$. If N_T is just a few particles, say, 100, the simulation will be poor, but as N_T becomes large (greater than 100,000), the simulation will be a very close approximation to the deterministic solutions to the Markov model differential equations for the "early time" portion of the simulation. As the probability approaches unity, the population of particles not residing in the absorbing state approaches zero, and the waiting time stochastic sampling process from a small "live" population has more inherent error, and the simulation becomes poor even though N_T is large.

Results and Conclusions: The Monte Carlo simulation code is applied to a representative nuclear reactor shutdown system (SCRAM) and compared with a deterministic solution of the FMSV model of the same problem (Fig. 6). For failure probability vectors within $0 < P_f(t) < 0.3$, the simulation is quite accurate. Because the "active particle" population becomes smaller as $P_f(t) \rightarrow 1$, calculation accuracy is diminished. Bias sampling techniques should overcome this problem. The important conclusions of the simulation are:

1. Time-dependent failure rates or nonlinear dependencies are easily simulated.
2. Failure rate coupling (degradation-healing) mechanisms can be described.
3. A synergism between fault tree analysis and Markov model analysis is achieved.

Importance to System Safety: Generic fault trees capable of including common cause/common mode dependencies can be used in a synthesis of smaller subsystems to approximately calculate the expected lifetime of the system. Rate dependent degradations (or healings) not currently represented by fault tree analysis can be assessed.

References

1. M. L. Shooman, Probabilistic Reliability: An Engineering Approach (McGraw-Hill, New York, 1968), pp.61-67, 96-115.

2. R. J. Bartholomew, "A State Space Method of Fault Tree Analysis with Applications," Los Alamos National Laboratory report LA-10298-T (December 1984).

3. F. G. Yost, I. J. Hall, "Failure by the Processes of Nucleation and Growth," IEEE Trans. on Reliability 25, 45-48 (1976).

Biography

Robert J. Bartholomew received the BSME from New Mexico State Univ., 1950; MS Engr. Mech., Univ. of Mich., 1954; MS, Nuclear Engr., Univ. of New Mexico, 1979; Ph.D., Nuclear Engr., Univ. of New Mexico, 1984. He is currently a Staff Member at the Los Alamos National Laboratory in the Design Engineering Division assigned to the Analysis and Testing Group. His background includes a diversified career in Engineering Analysis in the Aerospace industry. His more recent assignments involved safety analysis including nuclear criticality safety, and nuclear design and reliability systems analysis for advanced nuclear power systems.